Claims 1-6 and 13-24 are not obvious over *Moran* (US 6,647,400) in view of *Flint et al.* ("*Flint*")(US 6,453,419)

The 35 U.S.C. §102(a) rejection of claims 1-6 and 13-24 over *Moran* in view of *Flint* is respectfully traversed.

Independent claim 1 recites a method of detecting critical file changes, comprising, *inter alia*, reading an event representing at least one system call, "wherein the event is a kernel audit record read from an intrusion detection data source (IDDS)."

The U.S. Patent and Trademark Office (PTO) admits that *Moran* fails to disclose that the event representing a system call is a kernel audit record read from an intrusion detection data source (IDDS). The PTO relies upon *Flint* to remedy the deficiencies of *Moran*, asserting that because *Flint* discloses a system that sends kernel log messages to the audit subsystem in order to form filters (*Flint*, column 11, lines 19-45), it would be obvious to use the system of *Moran* to search the kernel audit logs as well. Applicants respectfully disagree.

First, *Moran*, at column 7, line 65 – column 8, line 1, appears to disclose a system "capable of reviewing data and identifying and characterizing intrusions after the fact." (Emphasis added). Notwithstanding the lack of explicit or implicit disclosure of all claimed elements in the combined disclosure of *Moran* and *Flint*, Applicants respectfully submit that the disclosures of *Moran* and *Flint*, taken as a whole, do not suggest Applicants' claimed system. Furthermore, the USPTO's Board of Patent Appeals and Interferences has stated that:

> "[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." (*In re Kahn*, 441 F. 3d 977, 988 (CA Fed. 2006) cited with approval in *KSR Int'l Co. v. Teleflex Inc.*, 127 S. Ct. 1727, 82 USPQ2d 1385).

The term "event" as recited in the claims, has been given a clear definition in the specification of co-pending patent application "COMPUTER ARCHITECTURE FOR AN INTRUSION DETECTION SYSTEM," filed June 12, 2001, U.S. Serial No. 09/878,320, the entirety of which has been incorporated into the instant specification by reference. Specifically, in paragraph [0154] of the published copending application, under the heading "ECS

Terminology," the term "event driven" means that events arriving, e.g., at the engine core, trigger processing. Applicants respectfully submit that neither *Moran* nor *Flint* teach or disclose the claimed "reading an event representing at least one system call, wherein the event is a kernel audit record read from an intrusion detection data source (IDDS). For at least this reason, withdrawal of the rejection is respectfully requested.

Second, as acknowledged by the PTO, *Flint* reads kernel logs to form filters. Nowhere does *Flint* disclose, teach, or suggest detecting critical file changes using a kernel audit record from an IDDS, as recited in claim 1. Furthermore, nowhere does *Moran* disclose, teach, or suggest, creating filters from logs. Applicants respectfully submit, therefore, that modifying *Moran* to read audit logs for any other purpose except generating filters would be an improper combination or modification of references. For at least this reason, withdrawal of the rejection is respectfully requested.

Based on at least the foregoing reasons, the combination of *Moran* and *Flint* fails to disclose, teach or suggest each limitation recited in amended claim 1. Therefore, claim 1 is patentable over *Moran* and *Flint*, and the rejection is respectfully requested to be withdrawn.

Claims 2-6, 21, and 23 depend, either directly or indirectly, from claim 1, include further features, and are patentable over the asserted combination of references for at least the reasons advanced above with respect to claim 1.

Claim 21

Specifically regarding claim 21, claim 21 recites determining a subdirectory of a directory based on an event and outputting the event for each event indicating a modification to the determined subdirectory. The PTO asserts that *Moran*, at column 9, lines 33-47, discloses this feature. Applicants respectfully disagree.

At the cited passage, *Moran* appears to only disclose a method to "monitor the effective User ID of processes for changes to privileged status that do not pass through the expected sequences." Nowhere does *Moran* appear to disclose the subject matter of claim 21. *Flint* likewise fails to disclose any reference made to an event indicating a modification to a determined subdirectory.

Claim 23

Regarding claim 23, the passages cited by the PTO (*Moran*, column 13, lines 35-42, and column 9, lines 33-47) relate to a "data-driven" system and not to an "event driven" system which includes "reading an event from an event-driven correlation service of the IDDS," as defined by copending Patent Application Serial No. 09/878,320.

Accordingly, Applicants respectfully submit that the rejection of claims 2-6, 21, and 23 should be withdrawn.

Claim 14

Claim 14 is patentable over *Moran* in view of *Flint* for at least reasons similar to those advanced above with respect to claim 1 and the rejection is respectfully requested to be withdrawn.

Claims 15-20, 22, and 24

Claims 15-20, 22, and 24 depend, either directly or indirectly, from claim 14, include further features, and are patentable over the applied art for at least the reasons advanced above with respect to claim 14. Furthermore, claims 22 and 24, system claims based upon the subject matter of method claims 21 and 23, are likewise allowable over the applied art. Withdrawal of the rejection of these claims is respectfully requested.

In view of the foregoing, it is respectfully submitted that this application is in condition for allowance. Favorable reconsideration and prompt allowance of claim 1-6 and 13-24 are earnestly solicited.

Conclusion

All objections and rejections having been addressed, it is respectfully submitted that the present application should be in condition for allowance and a Notice to that effect is earnestly solicited.

To the extent necessary, a petition for an extension of time under 37 C.F.R. 1.136 is hereby made. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 08-2025 and please credit any excess fees to such deposit account.

Respectfully submitted,

Mark Crosbie

Randy A. Noranbrock
Registration No. 42,940
Telephone: (703) 684-1111

HEWLETT-PACKARD COMPANY
IP Administration
Legal Department, M/S 35
P.O. Box 272400
Fort Collins, CO 80528-9599
Telephone: (970) 898-7057
Facsimile: 281-926-7212
Date: **November 1, 2007**
RAN/ERM